REMARKS

This application has been reviewed in light of the Office Action dated September 20, 2005. Claims 1-8 are presented for examination. Claims 1-8 have been amended to define still more clearly what Applicant regards as his invention. Claims 1, 6, and 8 are in independent form. Favorable reconsideration is requested.

Claims 1 and 5 were rejected under 35 U.S.C. § 112, second paragraph, as being indefinite. These claims have been carefully reviewed and amended as deemed necessary to ensure that they conform fully to the requirements of Section 112, second paragraph, with special attention to the points raised on page 2 of the Office Action. Specifically, the terminology in claims 1 and 5 have been amended to ensure consistency of terminology.

It is believed that the rejections under Section 112, second paragraph, have been obviated, and their withdrawal are therefore respectfully requested.

Claim 1 was rejected under 35 U.S.C. § 102(e) as being anticipated by U.S. Patent Publication No. 2002/0071562 (Parenty).

Claims 2, 3, 4/1, 4/2, 4/3 and 6 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Parenty in view of U.S. Patent No. 6,038,549 (Davis et al.)

Claims 5/1, 5/2, 5/3, and 8 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Parenty and U.S. Patent No. 6,629,150 (Huded) an in further view of U.S. Patent No. 6,226,618 (Downs et al.).

Claim 7 was rejected under 35 U.S.C. § 103(a) as being unpatentable over Parenty and Davis et al. and in further view of Huded and Downs et al.

As shown above, Applicant has amended independent Claims 1, 6, and 8 in terms that more clearly define the present invention. Applicant submits that these amended independent claims, together with the remaining claims dependent thereon, are patentably distinct from the cited prior art for at least the following reasons.

The rejection of claim 1 as being anticipated by Parenty will be discussed first.

Claim 1 is directed to a method for cryptographing information between a client terminal and a server which are connected to each other through a network. The method includes generating, at the server, a public key a private encryption key by driving an encryption module for encryption information to an access request from the client terminal, and sending, at the server, to the client terminal the public key and an encryption execution module including a message digest module for an integrity verification and a data compression module for reduction of transmission data and a double security by being

included in a Web document for user input in the form of a Java applet. The method further includes sending, at the client terminal, to the server an encryption message including a result of compressing an original message generated by encrypting information entered from a client through the encryption execution module sent form the server and a digest message digesting the original message, and including an encryption compression key encrypted with the public key, and upon receipt of the encryption message from the client terminal, decrypting, at the server, the encryption compression key by calling the private encryption key, decompressing the compressed result with the decrypted encryption compression key, and decrypting the original message with the private encryption key according to a result of the integrity verification.

A feature of claim 1 is sending to the client terminal the public key and an encryption execution module including a message digest module for an integrity verification and a data compression module for reduction of transmission data and a double security by being included in a Web document for user input in the form of a Java applet. That is, the encryption execution module for actually encryption processing at the client terminal is inserted into a Web page in the form of a Java applet and sent to the client terminal from the server. At the client terminal, the encryption execution module is executed using the RAM, volatile memory, to perform the encryption, not installed on the client terminal. As such, the encryption execution module is automatically removed from the RAM after execution of the encryption process and powering off the client terminal.

Parenty, as understood by Applicant, relates to a method and system for encrypting shared documents for transit and storage. In the Parenty method, a Java encryption applet and an EEC public key are sent from the encryption server system 100 to the client system 200 according to a request from the client system 200 (shown in Figures 1 and 2). The sent Java applet is then installed on the client system 200. Parenty states at paragraph 0034 that once the Triple DES symmetric key has been encrypted, at step 530, the execution of the Java encryption applet by the client may further includes the step of deleting the encryption server system EEC public key from any storage medium under the control of the client system 200. In the Parenty system, an installed method is used in which the encryption program is installed on a non-volatile memory, such as a hard disk, and the encryption program is deleted according to a control of the client system 200.

In contrast, the invention defined in claim 1 utilizes a non-installed method (see specification at page 22, lines 5-7) in which the encryption execution module sent from the server resides on the RAM of the client terminal for performing encryption and is

automatically deleted from the RAM by turning off of a power supply or working conditions of the client terminal.

Nothing has been found in Parenty that teaches or suggests sending to the client terminal the public key and an encryption execution module including a message digest module for an integrity verification and a data compression module for reduction of transmission data and a double security by being included in a Web document for user input in the form of a Java applet, as recited in claim 1.

For at least the above reason, Applicant submits that claim 1 is not anticipated by Parenty, and respectfully requests withdrawal of the rejection under 35 U.S.C. § 102(e).

The rejection of claim 6 as being unpatentable over by Parenty and Davis et al. will now be discussed.

Claim 6 is directed to a method for cryptographing information between a gateway communicating with a wireless terminal and a computer connected to the gateway. The method includes generating, at the computer, a public key and a private encryption key by driving an encryption module for information encryption according to an access request from the wireless terminal through the gateway, and sending, at the computer, to the wireless terminal through the gateway public key, and an encryption execution module including a message digest module for an integrity verification and a data compression module for reduction of transmission data and double security by being included in a Web document for user input in the form of a Java applet. The method also includes sending, at the wireless terminal, to the computer through the gateway an encryption message including a result of compressing an original message generated by encrypting information entered from a client through the encryption execution module sent from the computer and a digest message digesting the original message, and including an encryption compression key encrypted with the public key, and upon receipt of the encryption message from the wireless terminal through the gateway, decrypting, at the computer, the encryption compression key by calling the private encryption key, decompressing the compressed result with the decrypted encryption compression key, and decrypting the original message with the private encryption key according to a result of the integrity verification.

A feature of claim 6 is sending to the wireless terminal through the gateway public key, and an encryption execution module including a message digest module for an integrity verification and a data compression module for reduction of transmission data and double security by being included in a Web document for user input in the form of a Java applet.

For reasons substantially similar to those discussed above with respect to claim 1, nothing has been found in Parenty that teaches or suggests sending to the wireless terminal through the gateway public key, and an encryption execution module including a message digest module for an integrity verification and a data compression module for reduction of transmission data and double security by being included in a Web document for user input in the form of a Java applet, as recited in claim 6.

For at least this reason, Applicant submits that claim 6 is clearly patentable over Parenty.

Davis et al., as understood by Applicant, relates in general to selective call signaling systems and more particularly to a selective call signaling system that facilitates secure financial transactions over a wireless network using a portable 1-way financial messaging unit. Davis is cited in the Office Action as teaching the use of wireless terminals.

However, nothing has been found in Davis et al. that teaches or suggests sending to the wireless terminal through the gateway public key, and an encryption execution module including a message digest module for an integrity verification and a data compression module for reduction of transmission data and double security by being included in a Web document for user input in the form of a Java applet, as recited in claim 6.

Applicant submits that a combination of Parenty and Davis et al., assuming such combination would even be permissible, would fail to teach or suggest sending to the wireless terminal through the gateway public key, and an encryption execution module including a message digest module for an integrity verification and a data compression module for reduction of transmission data and double security by being included in a Web document for user input in the form of a Java applet, as recited in claim 6.

Accordingly, Applicant submits that claim 6 is patentable over Parenty and Davis et al., whether considered separately or in combination, and respectfully requests withdrawal of the rejection under 35 U.S.C. § 103(a).

The rejection of claim 8 as being unpatentable over by Parenty, Huded, and Downs et al. will now be discussed.

Claim 8 is directed to A method for cryptographing information between a wired/wireless client terminal and an encryption server, which is executed in a wired/wireless terminal. The method includes accessing the encryption server, downloading a public key, and an encryption execution module including a message digest module for an integrity verification and a data compression module for reduction of transmission data and double security from the encryption server in a non-installed manner, encrypting information entered

from a client with the public key by executing the downloaded encryption execution module to generate an original message, and digesting the encrypted original message by the message digest module. The method also includes compressing the original message and the digested original message with an encryption compression key generated by randomly extracting a part of the public key, encrypting the encryption compression key with the public key having been used to encrypt the original message, and converting the compressed original message, the compressed digested original message and the encrypted encryption compression key into a Web document file, and sending the Web document file to the encryption server.

A feature of claim is downloading a public key, and an encryption execution module including a message digest module for an integrity verification and a data compression module for reduction of transmission data and double security from the encryption server in a non-installed manner.

As discussed above, with respect to claim 1, Parenty utilizes an installed method is used in which the encryption program is installed on a non-volatile memory, such as a hard disk. However, nothing has been found in Parenty that teaches or suggests ownloading a public key, and an encryption execution module including a message digest module for an integrity verification and a data compression module for reduction of transmission data and double security from the encryption server in a non-installed manner.

For at least this reason, Applicant submits that claim 8 is patentable over Parenty, taken alone.

The Office Action cites Huded as teaching compressing the original message and the digested original message with an encryption compression key under the condition that the encryption key is generated by randomly extracting a part of the public key. Huded, as understood by Applicant, relates to a method for preventing digital information from unauthorized observation, manipulation and/or distribution by users, applications, and machines. However, nothing has been found in Huded that teaches or suggests downloading a public key, and an encryption execution module including a message digest module for an integrity verification and a data compression module for reduction of transmission data and double security from the encryption server in a non-installed manner, as recited in claim 8.

For at least this reason, Applicant submits that claim 8 is patentable over Huded, taken alone.

The Office Action cites Downs et al. as teaching digesting the encrypted original message, encrypting the encryption compression key with the public key having been used to encrypt the original message and compressed converting the compressed original message,

the digested original message and the encrypted encryption compression key into Web documents and sending the Web documents. Downs et al., as understood by Applicant, relates to a system and related tools for the secure delivery and rights management of digital assets, such as print media, films, games, and music over global communications networks such as the Internet and the World Wide Web. However, nothing has been found in Downs et al. that teaches or suggests downloading a public key, and an encryption execution module including a message digest module for an integrity verification and a data compression module for reduction of transmission data and double security from the encryption server in a non-installed manner, as recited in claim 8.

For at least this reason, Applicant submits that claim 8 is patentable over Downs et al.

Accordingly, Applicant submits that claim 6 is patentable over Parenty, Huded, and Downs et al., whether considered separately or in combination, and respectfully requests withdrawal of the rejection under 35 U.S.C. § 103(a).

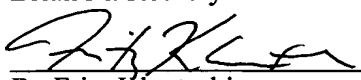
The other rejected claims in this application depend from one or another of the independent claims discussed above, and, therefore, are submitted to be patentable for at least the same reasons. Since each dependent claim is also deemed to define an additional aspect of the invention, individual reconsideration of the patentability of each claim on its own merits is respectfully requested.

In light of the above amendments and remarks, Applicant respectfully requests that the Examiner reconsider this application with a view towards allowance. The Examiner is invited to call the undersigned attorney if a telephone call could help resolve any remaining items.

Respectfully submitted,

Date: January 20, 2006

35,340
Brian M. Rothery (Reg. No.)



50,333
By Fritz Klantschi (Reg. No.)

JONES DAY
222 East 41st Street
New York, New York 10017
(212) 326-3939